ARMIS®

WHITE PAPER

The State of Cybersecurity in Airports

Introduction

Airports are bustling hubs, overseeing thousands of interconnected operations each day. Historically, airport security measures focused on physical threats, such as terrorism and smuggling. However, the evolving threat landscape has introduced a new breed of adversaries aiming to exploit vulnerabilities in airport systems. Cyber threats targeting airports are vast and complex, with attacks from various sources, including state-sponsored hackers, criminal groups, and insiders with access to sensitive information. These attacks can take many forms, such as phishing, malware, ransomware, or denial of service (DoS) attacks.

Every function within an airport relies heavily on interconnected systems, making them attractive targets for cybercriminals. Recent news headlines show how a failure in one part of the system can ripple throughout the travel process and bring airport operations to a standstill. Last year, a software update shut down passenger check-in and screening checkpoints at multiple airports and grounded flights at major airlines throughout the United States. In September, a ransomware attack on an international airport caused an internet outage that disrupted reservation check-in systems, flight information display screens, baggage-sorting systems, and phone service.

Understanding the current trends and challenges in airport cybersecurity is paramount for maintaining the safety and efficiency of air travel.

The Broader Implications for Critical Infrastructure

The increase in severity and number of cybersecurity incidents underscores the fragile nature of airports and their susceptibility to cyber threats. Airports and airlines, as critical infrastructure, are prime targets for cyberattacks due to their dependence on complex networks of interconnected systems, including Information Technology (IT), Operational Technology (OT), and Internet of Things (IoT). IT systems encompass traditional computing and data processing. OT systems control cyber-physical operations like baggage handling and air traffic control, while IoT assets include sensors, cameras, and smart systems increasingly embedded within airport and airline infrastructure. The convergence of these technologies creates a highly interconnected environment, where a breach in one system can have cascading effects across the entire airport. Given the essential role that airports and airlines play in global transportation and trade, the consequences of a cyberattack can be far-reaching, impacting not only travelers, but also airlines, logistics, and supply chains. Such attacks highlight the need for airports and airlines to rethink their approach to cybersecurity, with a focus on visibility, security, and control over all assets.

Airports' Cyber Security Challenges

Cybersecurity in airports has become a pressing concern, with several key trends shaping the landscape:

Increasing Cyber Attacks: Airports are becoming prime targets for cyber breaches and attacks. Recent incidents, such as ransomware attacks on airport websites and data breaches affecting flight information screens, underscore the urgent need for robust cybersecurity measures.

Regulatory Pressure: The Transportation Security Administration (TSA) has introduced stringent cybersecurity requirements, pushing airports to adopt more rigorous protections. These regulations compel airports to upgrade their cybersecurity infrastructure and processes to comply with new standards.

Complex, Sprawling Network Environments: Airports are some of the most complex network environments, with numerous interconnected systems that serve diverse functions. Ensuring each segment remains isolated and protected against potential vulnerabilities is a significant challenge.

Asset Visibility & Behavior Monitoring

The Importance of Real-Time Visibility

In an environment as dynamic as an airport, real-time visibility into connected assets is crucial. Airports need to know what assets are present, their activities, and behavioral patterns to identify any anomalies. This visibility gap poses significant security risks, making asset discovery, analysis, and threat detection essential components of modern airport cybersecurity strategies.

> **Comprehensive Asset Inventory:** Airports must maintain an up-to-date inventory of all connected assets, including IT, OT, and IoT systems, both landside and airside. This inventory provides real-time insights essential for exposing risks and maintaining a secure environment.

> **Behavior Monitoring:** Monitoring asset behavior and identifying anomalies can help detect potential threats early. Unique multi-detection engines that include both active and passive discovery techniques to build a complete network map, including connections and traffic flows to/from other assets, virtual and physical segments, and external internet.

Regulatory Pressure

Compliance with TSA Requirements

Compliance with TSA requirements is crucial for ensuring the safety and security of travelers.

However, these requirements have often been a source of confusion for many airport security teams. The intricacies of security protocols and frequent updates to regulations can leave both passengers and airport staff struggling to keep up. Understanding this, the TSA is committed to collaborating closely with the airport industry. They aim to reach common ground in effectively meeting these requirements, while minimizing confusion. By fostering open communication and developing clear guidelines, the TSA and airport partners work together to streamline procedures, ensuring a smoother experience for all travelers.

The TSA's stringent cybersecurity requirements compel airports to adopt more rigorous protections. Key mandates include:

> **Network Segmentation:** Policies and controls to ensure operational technology systems can continue to operate safely even if an IT system is compromised.

> **Access Control Measures:** Securing and preventing unauthorized access to critical cyber systems.

> **Continuous Monitoring and Detection:** Policies and procedures to defend against, detect, and respond to cybersecurity threats and anomalies affecting critical cyber system operations.

> **Risk-Based Vulnerability Management:** Applying security patches and updates timely, using a risk-based methodology, to reduce the risk of exploitation of unpatched systems.

Increasing Cyber Attacks

Airports as Prime Targets

Airports have become lucrative targets for cybercriminals seeking high-impact outcomes. Attacks on critical infrastructure and OT systems can cause widespread disruption, making them appealing to attackers.

> **Ransomware Attacks:** The ability to halt operations, delay passenger and baggage screening, and cause public panic increases the likelihood of ransom payments and media attention.

> **Data Breaches:** Incidents affecting flight information screens and other critical systems highlight the need for proactive cybersecurity measures. Disruptions to critical infrastructure at airports not only stall the movement of travelers but also have cascading effects on global trade and security, highlighting the interconnectedness of air transport and commerce.

Resource Constraints

Challenges of Limited Resources

Many airports operate with limited resources, making it challenging to implement comprehensive cybersecurity measures. Staffing constraints further complicate their security posture, forcing them to balance efforts across landside and airside assets.

> **Cost-Effective Solutions:** Airports need scalable, cost-effective solutions that deliver robust security without overwhelming their operating resources. Smaller airports, in particular, face significant challenges due to limited budgets and personnel.

> **Automated Vulnerability Management:** With a high volume of vulnerability and security alerts, airports need automated systems to prioritize and operationalize remediation. This minimizes lag times between identifying, assigning, and fixing vulnerabilities.

Questions to Ask Yourself When Assessing Airport Security Posture

To address these challenges, airport security personnel, IT security companies, and regulatory authorities must consider the following questions:

- How do you discover connected assets in your environment, both landside and airside?
- Do you have a complete and up-to-date asset inventory, including all types such as IoT and cloud?
- When assessing vulnerabilities, do you have the necessary data on vulnerable assets, including type, exploit activity, location, and ownership?
- How do you prioritize and remediate vulnerabilities? Do you leverage early warning threat actor exploitation insights?
- How do you ensure all endpoints are protected by up-to-date security solutions?
- How quickly can you pinpoint and address impacted assets when a threat is detected?
- If you had a unified data view, would it improve your mean time to respond (MTTR)?

Steps Airports Can Take to Enhance Visibility, Security, and Control

Comprehensive Asset Inventory: Transportation and logistics operators must start by creating a detailed inventory of all IT, OT, and IoT assets connected to their networks. This includes everything from servers and workstations to baggage handling systems, surveillance cameras, and HVAC systems. Understanding the scope of their digital infrastructure and the interconnections between them is the first step toward securing it. Tools that offer automated discovery and continuous monitoring of assets can help ensure that no asset goes unnoticed.

Zero Trust Architecture: Adopting a Zero Trust approach to cybersecurity is essential in today's threat landscape. This means assuming that every asset, user, and application is a potential threat until proven otherwise. Airports and carriers should implement multi-factor authentication (MFA), identity and access management (IAM) solutions, and continuous monitoring to ensure that only authorized personnel and assets have access to sensitive systems, and only to the level their job requires.

Real-Time Monitoring and Threat Detection: Airports and airlines must deploy advanced threat detection systems that can monitor asset behavior, and network traffic in real-time, and identify suspicious activities. These systems should detect both known and unknown threats using techniques such as behavioral analysis, anomaly detection, and artificial intelligence/ machine learning. Early detection is key to mitigating the impact of a cyberattack and preventing widespread disruption.

Network Segmentation: Segmenting the network is crucial for containing potential breaches. By isolating critical systems, such as air traffic control and baggage handling, from less critical systems, airports can prevent a cyberattack from spreading across the entire network. Implementing strict access controls and limiting communication between segments can further reduce the risk of lateral movement by attackers.

Patch Management and Vulnerability Assessment: Keeping systems up-to-date with the latest security patches is a fundamental aspect of cybersecurity. Airports and airlines should implement a robust patch management process that ensures vulnerability detection, deduplication, prioritization, assignments, and timely updates to all software and firmware. Regular vulnerability and security assessments can help identify and address potential weaknesses in a "risk to business" prioritization before attackers can exploit them.

Incident Response Planning: A well-defined incident response plan is critical for minimizing the impact of a cyberattack. Airports and carriers should have a dedicated incident response team in place, with clear protocols for identifying, containing, and remediating threats. Regular drills and simulations can help ensure that staff are prepared to respond effectively in the event of a cyber incident.

Collaboration and Information Sharing: Airports and carriers should collaborate with government agencies, industry partners, and cybersecurity organizations to share information about emerging threats and best practices. One of the key sources includes The Cybersecurity & Infrastructure Security Agency (CISA) which works extensively with transportation and other critical infrastructure areas. Participation in threat intelligence sharing networks can help airports stay ahead of the latest cyber threats and strengthen their defenses.

Employee Training and Awareness: Human error remains one of the leading causes of cybersecurity breaches. The transportation and logistics industry must invest in regular training programs to educate employees about the latest cyber threats and the importance of following security protocols. Employees should be trained to recognize phishing attempts, suspicious links, and other common attack vectors.

Cyber-Physical Security Integration: Cybersecurity and physical security should be integrated to provide a holistic approach to protecting airport and airline infrastructure. This includes securing access to critical areas, such as server rooms and control centers, as well as monitoring physical access to IoT assets. Combining physical and cyber threat intelligence can provide a more comprehensive view of potential risks.

Resilience and Recovery Planning: In addition to preventing cyberattacks, airports must also focus on resilience and recovery. This includes developing backup systems, redundant communication channels, and disaster recovery plans that can help restore operations quickly in the event of a cyber incident. Regular testing of these plans is essential to ensure their effectiveness.

Real-life Examples

UNITED

United Airlines Uses Armis Centrix™ to Decrease OT Cybersecurity Risk

United Airlines, an industry leader in aviation, recognized the importance of strengthening their operational technology (OT) cybersecurity posture to protect against evolving threats. By implementing Armis Centrix™, United Airlines enhanced its ability to monitor, detect, and mitigate risks associated with OT environments. This innovative solution provided comprehensive visibility into unmanaged assets, a critical capability given the complexity and scale of airline operations.

With Armis Centrix™, United Airlines achieved better asset management and reduced the attack surface by identifying potential vulnerabilities and applying timely security measures. The solution's real-time monitoring and threat detection capabilities allow for the proactive identification of abnormal asset behavior, ensuring the security team can swiftly respond to potential threats. This approach not only fortified United Airlines' cybersecurity defenses, but also ensured compliance with regulatory standards governing critical infrastructure. This case study illustrates how leveraging advanced cybersecurity technologies can significantly enhance the security and resilience of airport and airline operations in an increasingly digital world.

Challenges

- Building a complete and accurate OT asset inventory
- Categorizing OT assets
- General need to decrease risk to the organization

Results

- Provided deeper visibility into the large OT asset estate
- Enhanced security posture
- Helped prepare for new regulation and compliance requirements
- Prioritized vulnerabilities for the incident response team

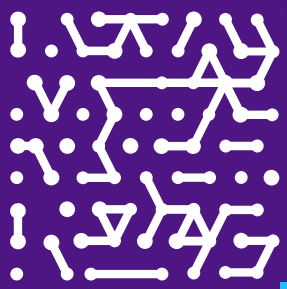
Conclusion

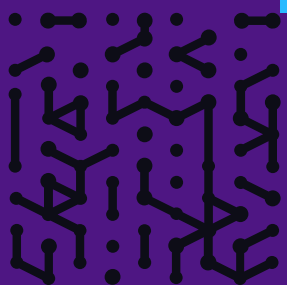
The rise in cyberattacks on passenger transport is a wake-up call for the aviation industry. As digitization increases, robust cybersecurity becomes urgent. Recent attacks should prompt global airports to strengthen cybersecurity. Securing critical infrastructure starts with a strong cyber asset attack surface management (CAASM) program.

Airports need a comprehensive approach with real-time visibility, threat detection, and compliance with regulations to improve security and protect infrastructure. Investing in advanced cybersecurity is essential for the safety, efficiency, and resilience of airport operations. The future of air travel depends on the combined efforts of security personnel, IT companies, and regulators to develop a robust cybersecurity framework.

Armis collaborates with airports, airlines, and logistics to enhance visibility, security, and control over devices to guard against threats. For more details on enhancing your airport's cybersecurity, contact us today.

Get Started with Armis Centrix™ Today





Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial